

## Poor leadership linked to insider security threat

A new study on IT security shows that many financial services firms are being compromised in their efforts to combat insider threat by poor leadership at executive level, a lack of accountability, and insufficient investment.

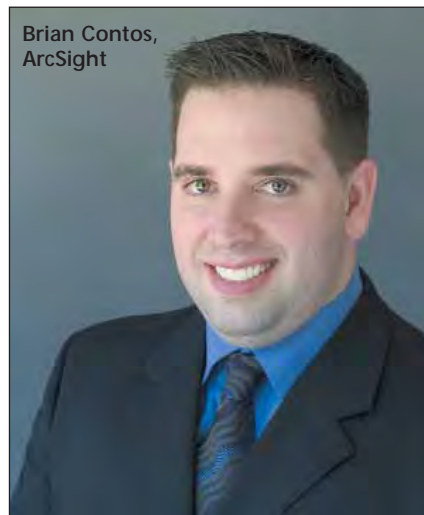
Researchers for the 'Managing the Insider Threats' study, by US-based privacy and information management firm, the Ponemon Institute, questioned 461 US-based heads of IT departments from a variety of businesses. Almost a quarter of the respondents currently function in the financial services market. Of all firms, over 80 per cent employ more than 5000 people and operate throughout North America, Europe, Asia Pacific and Latin America. Few claim to be immune from insider threat.

'While we seem to be inundated with reports of data breaches, we may not know the full extent of the problem,' admits the Institute's Larry Ponemon, commenting on the reasons for conducting the study. But the survey reveals that more than 78 per cent of respondents were aware of at least one insider-related security breach within their company. And with more than 55 per cent of respondents claiming that insider-related security problems represent more than 30 per cent of their company's overall risk management activities, it is clearly not to be taken lightly.

However, Brian Contos, chief security officer with US security technology vendor, ArcSight, struggles with the knowledge that doing something about the problem seems a little way down the agenda for many firms. Indeed, as the report shows, over 90 per cent of interviewees attributed increased insider risk to a lack of budget, time and headcount resources. Around 80 per cent stated that poor leadership was to blame for increased insider risk, with 31 per cent of them claiming that no one person in their company has overall responsibility for managing insider threats. 'Lack of resources and leadership makes it difficult to address insider threat,' suggests Ponemon. The situation, says Contos, may be related to a gap in perception of the threat between those at the sharp end – the IT department heads – and their CEOs. Almost 90 per cent of respondents believe

that insider threat poses a significant business risk for their companies. Only 49 per cent of CEOs share their concern.

Where insider threat has hit home, the most significant negative impact it presents is in the subsequent remediation effort, with 35 per cent of the vote. A further 16 per cent complain of the associated costs of incident response and investigations. The report calculates that the extrapolated average annual cost impact associated with insider-related security risks is \$3.4 million. It adds that the average investment in preventative measures is around \$1 million.



Brian Contos,  
ArcSight

Looking at security issues in general, a combination of manual controls and technologies are typically employed in an effort to contain breaches. Insider threats and missed or failed security patches are ranked as the top two known IT security risks. Technological attacks, such as viruses, hackers and Denial of Service attacks, are listed in the top six enterprise security risk list, but although on the increase, they tend to be fended off by improving technology, according to Contos. 'It tends to balance out in the end.'

Where insider threats were noted, the majority (66 per cent) cited carelessness and negligent staff as being mostly at fault. And where employee carelessness or lack of knowledge of procedure is evident, the most likely negative outcome is accidental data leakage, with around 60 per cent of respondents stating this occurs frequently or very frequently.

Unhappy or angry staff, those whose contracts had been terminated, and even temporary staff were identified as the next greatest risk set, with around 20 per cent each. The paper cites 48 per cent of respondents as reporting that corporate sabotage occurs frequently or very frequently because employees are angry or disgruntled, with 28 per cent saying that fraud occurs frequently or very frequently because of malicious employees.

Strangely, almost 60 per cent of respondents believe insider-related problems are more likely to occur outside of their own departments or organisational units. 'I don't think they're in denial,' jokes Contos, suggesting that the correct reading of this statement has more to do with a culture of silence and an unwillingness to expose any weakness than an outright refusal to believe there may be an internal problem. He adds that this may go some way to explaining why so many are aware of one or more breaches having occurred, yet do not necessarily feel able to report it.

Both Contos and Ponemon warn that companies need to appoint a single point of control for internal security, improve staff training and dissemination of policies, and open up on internal communication more readily if insider threat is to be addressed. 'It's not about spying on your colleagues,' Contos insists, 'it is more about the greater good of the business'.